doi: 10.3389/fict.2014.00003

Understanding computer security

***Sandro Etalle*[1,2]* and *Nicola Zannone*[1]**

[1] *Eindhoven University of Technology, Eindhoven, Netherlands*
[2] *University of Twente, Enschede, Netherlands*
**Correspondence: s.etalle@tue.nl*

Edited and reviewed by:
Frank Piessens, Katholieke Universiteit Leuven, Belgium

Keywords: computer security, accountability, privacy, monitoring, economics of security

INTRODUCTION

Few things in society and everyday life have changed in the last 10 years as much as the concept of security. From bank robberies to wars, what used to imply a great deal of violence is now silently happening on the Internet. Perhaps more strikingly, the very idea of privacy – a concept closely related to that of individual freedom – is undergoing such a profound revolution that people are suddenly unable to make rational and informed decisions: we protested for the introduction of RFID tags (Kelly and Erickson, 2005; Lee and Kim, 2006) and now we throw away *en-masse* most of our private information by subscribing to services (social media, free apps, cloud services), which have their reason of existence in the commerce of intimate personal data.

The ICT revolution has changed the game, and the security paradigms that were suitable for people and systems just up to 10 years ago are now obsolete. It looks like we do not know what to replace them with. As of today, we keep patching systems but we do not understand how to make them reasonably secure (Rice, 2007); perhaps more importantly, we do not understand what reasonable privacy guarantees are for human beings, let alone how to enforce them. We do not understand how to combine accountability and freedom in this new world, in which firewalls and digital perimeters cannot guarantee security and privacy any longer.

We believe that the root of the challenge that we face is *understanding security* and how information technology can enable and support such an understanding.

And just like security is a broad, multidisciplinary topic covering technical as well as non-technical issues, the challenge of understanding security is a multifaceted one, spanning across a myriad of noteworthy topics. Here, we mention just three that we consider particularly important.

UNDERSTANDING WHAT HAPPENS IN SYSTEMS (MONITORABILITY)

Our software is buggy, leaving the door open to cyberthreats. From what we see, we believe it will stay so for many years, leaving us in the hands of security technology, which is clearly not able to cope with the complexity of today's attacks. Advanced malware, advanced persistent threats, and alike are evading present countermeasures (mainly based on blacklisting) with discouraging ease. We still defend cyberassets using preventive measures such as access-control, firewalls, DMZs, and alike. These measures, however, are no match for a well-done targeted attack. The challenge is to discover the attack as soon as possible, and to limit the damages that it can do. Knowing that no blacklisting systems will recognize them, one is left with the task of detecting them as an anomaly in the normal system behavior. We are starting to see the first successes, based on, for instance, emulation (Lanzi et al., 2010). However, with hosts running hundreds of processes, internal networks producing gigabytes of traffic per hour, and log files that are megabytes long, finding the right anomaly is really like finding the proverbial needle in the haystack. Therefore, having given up the illusion that software will ever be completely bug-free, we believe that in the future, we will have software that is *monitorable by design*, software that facilitates the work of the security officers in detecting and reacting timely to threats.

UNDERSTANDING HOW TO BALANCE PRIVACY AND ACCOUNTABILITY

The last years have seen an increase in the tension between privacy and accountability (Anderson, 2014). We have witnessed (and accepted) a dramatic increase in online monitoring and surveillance. The NSA revelations (The Guardian, 2014) look almost like a logical consequence of this. The time when the Internet was meant to be "completely free" seems long gone, and while it is unacceptable for the Internet to be a free playground for criminals, creating a surveillance state will not solve the problem, but is creating a different – possibly larger – problem instead (Kehl et al., 2014). This is by no means a purely regulatory problem: it raises very hard technical challenges. In particular: how to make people accountable for their actions without putting at risk their privacy is a tremendously difficult technical problem, a problem that we are obligated to solve. The challenge is to allow people and institutions to keep control on their data, even when the data have left the premises of the personal computer, allowing people to mitigate mistakes while keeping them accountable when they cross the line. We have witnessed some important steps in this direction, particularly in the area of cloud computing (e.g., Takabi et al., 2010; Ko et al., 2011; Guagnin et al., 2012), but we believe that there is still a long way to go.

UNDERSTANDING THE VALUE OF SECURITY

Security has costs for people and organizations alike. Securing systems and data takes time, resources, money, and makes systems less usable. Today, IT-risk management is an art, not a science. Even companies with well-developed security systems are not able to properly "quantify" the costs and benefits of security and nor are they fully aware of the real consequences of security incidents. Risk-assessment standards (e.g., ISO/IEC 27001, NIST SP 800-30) give us very little support in understanding the trade-offs between benefits and often hidden costs. When we shift the focus from

organizations to people, this issue becomes even more pressing: people do not have the means to understand how much (the lack of) privacy and security could cost them. We do not know how much are we actually sacrificing in the name of functionality, services, usability, and lower direct costs. Strikingly, the – dual – *value of insecurity* is an area in which a lot of progress has been made recently. This relates to the offensive side of cybersecurity, where software vulnerabilities have now their own market, and a precise price list (Schneier, 2013a,b). The challenge for us remains to be able to quantify what is the *value of cybersecurity*; in particular, the challenge is to develop novel IT-risk assessment methods to support a person (or a company) in making decisions regarding the security and privacy measures to be taken. The research community is becoming aware of the urgency of such methods, and we can now find forums like Workshop on the Economics of Information Security (WEIS), that aim to bring together researchers and practitioners in order to advance the states of the art and practice in the evaluation of security.

Bringing our IT infrastructure to a reasonable security level is a tremendous challenge that we are facing now. It is a technological challenge with an important multidisciplinary component, touching economical, sociological, psychological, and regulatory issues. To tackle it properly, we will have to rethink some of the basic assumptions in computer security and solve a number of compromises, often spanning across more than one discipline.

REFERENCES

Anderson, R. J. (2014). "Privacy versus government surveillance where network effects meet public choice," in *Proc. 13th Annual Workshop on the Economic of Information Security (WEIS 2014)*, ed. J. Grossklags. Available at: http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf

Guagnin, D., Hempel, L., Ilten, C., Kroener, I., Neyland, D., and Postigo, H. (eds). (2012). *Managing Privacy through Accountability*. Palgrave Macmillan.

Kehl, D., Bankston, K., Greene, R., and Morgus, R. (2014). *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity. Policy Paper, New America's Open Technology Institute.* Available at: http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf

Kelly, E. P., and Erickson, G. S. (2005). RFID tags: commercial applications v. privacy rights. *Ind. Manag. Data Syst.* 105, 703–713. doi:10.1108/02635570510606950

Ko, R., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., et al. (2011). "TrustCloud: a framework for accountability and trust in cloud computing," in *Proc. 2011 IEEE World Congress on Services (SERVICES)* (Washington, DC: IEEE Computer Society), 584–588.

Lanzi, A., Balzarotti, D., Kruegel, C., Christodorescu, M., and Kirda, E. (2010). "Accessminer: using system-centric models for malware protection," in *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010* (Chicago, IL: ACM), 399–412.

Lee, H., and Kim, J. (2006). "Privacy threats and issues in mobile RFID," in *Proc. 1st International Conference on Availability, Reliability and Security* (Vienna, Austria: IEEE Computer Society), 510–514.

Rice, D. (2007). *Geekonomics: The Real Cost of Insecure Software.* Addison Wesley Publishing Company.

Schneier, B. (2013a). *Disclosing vs. Hoarding Vulnerabilities.* Available at: https://www.schneier.com/blog/archives/2014/05/disclosing_vs_ h.html

Schneier, B. (2013b). *The US Uses Vulnerability Data for Offensive Purposes.* Available at: https://www.schneier.com/blog/archives/2013/06/the_us_uses_vul.html

Takabi, H., Joshi, J., and Ahn, G.-J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Secur. Priv.* 8, 24–31. doi:10.1109/MSP.2010.186

The Guardian. (2014). *The NSA Files.* Available at: http://www.theguardian.com/world/edwardsnowden

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Received: 03 October 2014; accepted: 09 October 2014; published online: 22 October 2014.

Citation: Etalle S and Zannone N (2014) Understanding computer security. Front. ICT ***1****:3. doi: 10.3389/fict.2014.00003*

This article was submitted to Computer and Network Security, a section of the journal Frontiers in ICT.